UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

PAUL BENDER, on behalf of himself and all others similarly situated, Plaintiff, v. **COINBASE GLOBAL, INC. AND COINBASE, INC.,** Defendants.	Case No. _____ CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Paul Bender ("Plaintiff"), on behalf of himself and all others similarly situated, upon personal knowledge of facts pertaining to himself and on information and belief as to all other matters, by and through undersigned counsel, brings this Class Action Complaint against Defendants, Coinbase Global, Inc. and its subsidiary Coinbase, Inc. (collectively, "Coinbase" or "Defendants").

I. INTRODUCTION

1. This class action arises from Coinbase's failure to protect the sensitive personal information of millions of users, including current and former customers. Despite collecting and storing extensive personal and financial data as part of its cryptocurrency services, Coinbase failed to implement and maintain reasonable security safeguards, thereby exposing users to serious and ongoing risks.

2. On May 15, 2025, Coinbase publicly disclosed in a regulatory filing with the U.S. Securities and Exchange Commission (Form 8-K) that it had been contacted by a malicious actor who claimed to have obtained a wide array of confidential user information. According to the threat actor's communication on May 11, 2025, the stolen data included names, physical and email

addresses, phone numbers, partial Social Security numbers, account login credentials, banking information, copies of government-issued identification, and records of user activity on the platform ("Private Information" or "PII").

3. Coinbase—one of the largest and most well-capitalized digital asset platforms in the world—possesses the technical and financial resources to implement industry-standard cybersecurity protections. Yet Coinbase failed to adopt even the most basic safeguards, such as properly and adequately encrypting sensitive data, timely application of security patches, and employee access controls, thereby breaching its duty to safeguard user information.

4. This breach was not the result of a sophisticated or unforeseeable attack, but rather a consequence of Coinbase's grossly inadequate security posture. On information and belief, the company's systems lacked real-time monitoring and failed to detect the intrusion for days. The company's response was delayed and insufficient, compounding the damage and leaving victims vulnerable to identity theft, financial fraud, and unauthorized access to their accounts.

5. As a result of Coinbase's failures, Plaintiff brings this action on behalf of all individuals whose personal information was compromised. Plaintiff seeks relief including compensatory damages, restitution, injunctive relief requiring improved data security measures, and disgorgement of profits obtained through Coinbase's negligent and unlawful practices.

II. JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The proposed class consists of more than 100 members, the amount in controversy exceeds $5,000,000 exclusive of interest and costs, and minimal diversity exists because at least one putative class member is a citizen of a state different from that of Defendants.

7. This Court has personal jurisdiction over Defendants because Coinbase maintains

its principal place of business in New York City and purposefully conducts substantial business within this District. By offering and providing cryptocurrency services to residents of New York, Coinbase has expressly availed itself of the privilege of conducting activities within the state, thereby invoking the benefits and protections of its laws.

8. Venue is proper in this District under 28 U.S.C. § 1391(b) because Coinbase's principal place of business is located in this District, Coinbase transacts business extensively here, and a substantial portion of the acts and omissions giving rise to the claims occurred within this District.

III. PARTIES

Plaintiff

9. Plaintiff Paul Bender is a citizen of the state of New Jersey. Plaintiff Bender is a customer of Coinbase and has been since 2013.

Defendants

10. Defendant Coinbase Global, Inc. is a publicly traded holding company headquartered in New York City. As the parent corporation, Coinbase Global, Inc. oversees the operations, governance, and strategic direction of its subsidiaries, including Coinbase, Inc. Its principal executive offices are located at One Madison Avenue in Manhattan, a central hub of corporate and financial activity.

11. Defendant Coinbase, Inc. is a wholly owned subsidiary of Coinbase Global, Inc. and serves as the operational arm of the enterprise. Coinbase, Inc. provides a digital platform through which individuals can buy, sell, store, and trade cryptocurrency assets. It maintains extensive customer-facing infrastructure and is responsible for collecting and storing sensitive user information as part of its service offerings. Together, Coinbase Global, Inc. and Coinbase, Inc. operate one of the largest cryptocurrency exchanges in the world.

IV. FACTUAL ALLEGATIONS

A. The Data Breach and Defendants' Failure to Respond Adequately

12. On or around May 11, 2025, a cybercriminal contacted Coinbase to claim responsibility for a significant data breach involving the unauthorized access and exfiltration of confidential user data (the "Data Breach".) The actor asserted that they had obtained a substantial volume of PII belonging to Coinbase customers—an assertion Coinbase later confirmed.

13. In a May 15, 2025, Form 8-K filing with the U.S. Securities and Exchange Commission, Coinbase publicly disclosed the breach and revealed the potential scale of the incident. Coinbase stated that it anticipated incurring between $180 million and $400 million in expenses associated with breach remediation, forensic investigations, customer notification, legal exposure, and heightened security measures—a figure indicative of the extreme severity and scope of the incident.[1]

14. Despite the magnitude of the breach, Coinbase's immediate response was inadequate, fragmented, and delayed. Users were not promptly or fully informed of the compromise, and Coinbase did not immediately take meaningful steps to mitigate further harm, provide identity protection services, or offer actionable guidance to affected individuals.

15. On information and belief, the data accessed during the breach—including highly sensitive elements such as Social Security numbers, bank details, and government-issued identification—was stored by Coinbase in poorly protected formats. This conclusion is supported by the attacker's apparent ability to retrieve the information in a usable and unredacted state.

16. The nature and precision of the breach strongly suggest that Coinbase was intentionally targeted. As one of the most prominent cryptocurrency platforms globally, Coinbase

[1] Coinbase Glob. Inc., Current Report (Form 8-K) (May 15, 2025); see also Paul Vigna, *Coinbase Says Customer Data Stolen, Held for Ransom*, WALL ST. J. (May 15, 2025), https://www.wsj.com/finance/currencies/coinbase-global-says-customer-data-stolen-held-for-ransom-e5108336.

holds large volumes of sensitive user data, making it a prime target for financially motivated cybercriminals. The stolen PII can be used or sold to facilitate a range of identity-related crimes, including: opening unauthorized bank or credit accounts, applying for loans or benefits, filing fraudulent tax returns, obtaining false identification documents, and impersonating victims in interactions with law enforcement or financial institutions.

17. As a result of Coinbase's lax data security practices, Plaintiffs and Class members now face a substantial, immediate, and ongoing threat of identity theft and financial fraud. The consequences of the breach are long-term and potentially permanent, as the compromised information cannot be recovered or made secure once exposed.

18. Coinbase's failure to prevent this breach is especially egregious given the well-documented risks of cyberattacks targeting consumer financial platforms. Despite its expansive customer base and substantial financial resources.

19. Upon information and belief, Defendant failed to adequately encrypt or otherwise safeguard the sensitive PII that was accessed and exfiltrated in the Data Breach. To the extent Defendant claims to encrypt data in transit and at rest, such measures were either not in place or were ineffective in preventing unauthorized access.

20. Coinbase also failed to ensure that its personnel received adequate training in information security. Employees and contractors with access to sensitive data were not properly instructed on secure handling protocols, including limiting access based on role, securing endpoints, and adhering to company-wide guidelines on PII protection.

21. These failures led directly to the unauthorized disclosure of Plaintiffs' and Class members' private information to an external actor, who exploited vulnerabilities in Coinbase's systems to gain access without detection. The resulting exposure has placed victims at serious and continuing risk.

22. Coinbase's security failures represent a clear breach of its legal, contractual, and ethical obligations to safeguard customer data. The company ignored established cybersecurity standards and best practices promulgated by regulatory bodies, including the Federal Trade Commission (FTC), as well as guidelines widely adopted by the financial services industry.

23. Though Coinbase publicly markets itself as a technologically advanced platform, it neglected to implement baseline protections such as timely software patching, secure adequate encryption protocols, and robust access controls. These omissions reflect systemic neglect and prioritization of growth and profitability over user security.

24. Coinbase also failed to audit and train internal personnel—particularly those with privileged access to sensitive data—on applying critical security updates, detecting suspicious activity, and following operational protocols designed to prevent unauthorized access. This failure reflects a broader breakdown in Coinbase's internal governance and risk management practices.

B. Defendants' Collection of PII and Legal Duty to Safeguard this PII

25. As part of its core business operations, Coinbase, Inc. collects, stores, and processes a vast amount of PII from individuals who sign up to use its cryptocurrency exchange platform. This information includes names, dates of birth, physical and email addresses, phone numbers, government-issued identification documents, Social Security numbers, banking and payment details, and user transaction histories. Such data is obtained both during the onboarding of new users and throughout ongoing account activity.

26. Coinbase requires customers to submit this information as a condition of accessing its services, including for identity verification, fraud prevention, and compliance with financial regulations such as Know Your Customer (KYC) and anti-money laundering (AML) laws. In doing so, Coinbase represents—explicitly and implicitly—that it will safeguard the information using reasonable and industry-standard security measures.

27. By collecting and deriving commercial benefit from this PII, Defendants assumed legal, contractual, and equitable obligations to protect it. Coinbase had a duty to implement appropriate technical and administrative safeguards to ensure that customer data remained confidential, secure, and protected against unauthorized access, use, or disclosure.

28. Plaintiff and Class members reasonably relied on Coinbase's representations, public statements, privacy policies, and course of dealing to believe that their private information would be handled responsibly and stored securely. Coinbase's failure to maintain the confidentiality and integrity of this data—by exposing it through inadequate cybersecurity measures—violated that trust and breached its duties.

29. At all relevant times, Coinbase owed a duty to Plaintiff and Class Members to protect their PII from unauthorized access, theft, and disclosure. This duty arose from its role as a custodian of sensitive financial and identification data and encompassed the obligation to implement and maintain reasonable data security measures, train personnel on secure data practices, detect and respond to threats in real time, and promptly notify users upon discovering any breach of security.

30. Despite possessing substantial financial and technological resources, Coinbase failed to make adequate investments in cybersecurity infrastructure. It neglected to effectively deploy essential protections such as data encryption, network intrusion detection, endpoint monitoring, and rigorous access controls. This failure to safeguard PII constitutes a violation of Coinbase's obligations under common law, regulatory expectations, and industry best practices.

31. Security standards widely recognized in the financial and technology sectors for the protection of sensitive user data include, but are not limited to, the following:

a. Implementing internal access controls to ensure that employees and contractors can only access the specific data required to perform their job functions;

b. Establishing continuous monitoring and auditing protocols to detect and respond to unauthorized access or anomalous behavior in real time;

c. Deploying insider threat detection tools and behavior analytics to identify malicious or negligent actions by internal personnel;

d. Enforcing strict data access policies, including the principle of least privilege and role-based access controls, to reduce unnecessary data exposure;

e. Providing mandatory and ongoing employee training on information security best practices, phishing awareness, and social engineering defense;

f. Developing and maintaining a tested incident response plan, enabling prompt containment and mitigation of data breaches to prevent further data exfiltration.

32. While Coinbase states in its Global Privacy Policy—under the section titled "How We Protect Your Information"—that it encrypts sensitive information (such as financial data) both in transit and at rest, the effectiveness and adequacy of those security measures are called into question by the nature and scope of the Data Breach. Based on the breadth and apparent usability of the stolen data—including government-issued ID images, banking details, and partial Social Security numbers—it is reasonable to infer, upon information and belief, that either such information was not properly encrypted, or that the encryption was inadequate, improperly implemented, or bypassed due to insufficient access controls or internal security practices. The attackers' ability to exfiltrate and attempt to extort Coinbase using this data strongly suggests that Coinbase's data protection measures failed to prevent unauthorized access to highly sensitive information.

33. Despite the severity of the breach and the risks to affected users, Coinbase has not offered victims any form of credit monitoring, identity theft protection, or fraud resolution assistance. This omission stands in contrast to standard industry practices and reinforces the

perception that Coinbase is downplaying the seriousness of the breach.

34. By failing to provide post-breach support to its users, Coinbase has left millions of affected individuals to manage the fallout independently, despite the fact that they had no role in causing the breach. This response not only compounds the harm caused but also underscores Coinbase's failure to meet its responsibilities as a custodian of sensitive personal and financial information.

35. Coinbase was obligated—by contract, industry standards, and common law—to maintain the confidentiality of Plaintiff's and Class Members' PII and to protect it from unauthorized access. These obligations were reinforced by Coinbase's privacy policies and its public assurances that it employs strong security measures to protect user information.

36. This breach was entirely preventable with reasonable cybersecurity practices. Upon information and belief, Coinbase could have avoided or significantly limited the scope of the breach by implementing and maintaining appropriate security measures, including but not limited to: effective encryption of sensitive data, robust access controls (particularly for third-party contractors), timely software patching, and automated threat detection systems. Its failure to employ such safeguards—despite the highly sensitive nature of the data it collects and stores—directly contributed to the unauthorized access and exfiltration of Class Members' personal and financial information.

C. Coinbase's Failure to Protect PII Amid a Foreseeable Cybersecurity Threat Landscape

37. By collecting and using this data in the course of offering financial services and for its own commercial benefit, Coinbase assumed legal and equitable duties to protect such information from unauthorized access or disclosure.

38. Plaintiff and Class Members took reasonable steps to protect their own PII and entrusted Coinbase to uphold its promise and legal obligation to maintain the confidentiality and

security of that data.

39. Consumers place extraordinary value on the security and privacy of their personal information, especially when transacting on platforms handling digital currency. Identity theft resulting from data breaches causes immediate and long-term harm, including financial losses, reputational damage, credit impairment, emotional distress, and substantial time spent attempting to mitigate the consequences.[2]

40. Data breaches materially increase the risk of identity theft. According to the U.S. Department of Justice, identity theft results in both direct and indirect losses. Direct losses include stolen funds and fraudulent transactions, while indirect losses include legal fees, account restoration costs, and other out-of-pocket expenses such as postage, phone calls, or time off work to repair the damage.[3]

41. Plaintiff and Class Members are particularly concerned about the exposure of Social Security numbers, which serve as a critical key for identity verification across the U.S. financial and governmental systems. Once exposed, a Social Security number becomes a lifelong vulnerability.

42. Victims cannot simply replace their Social Security numbers. The Social Security Administration (SSA) has emphasized that a new number does not erase the consequences of identity theft, as existing records—including those held by the IRS, credit bureaus, and state agencies—remain linked to the compromised number.[4]

43. The SSA has further warned that changing a Social Security number is rarely a complete remedy, stating: "A new number probably won't solve all your problems," particularly

[2] Identity Theft Resource Center, *2022 Consumer Impact Report*, available at https://www.idtheftcenter.org.
[3] Bureau of Justice Statistics, *Victims of Identity Theft, 2016*, U.S. Department of Justice (NCJ 251147).
[4] Soc. Sec. Admin., *Can I Change My Social Security Number?*, SSA FAQ, https://faq.ssa.gov/en-us/Topic/article/KA-01981.

when other personal data such as names and addresses remain unchanged.[5] This leaves breach victims with no meaningful path to fully protect themselves.

44. The threat landscape is only worsening. According to the Identity Theft Resource Center, the U.S. experienced a record 1,862 reported data breaches in 2021, marking a 68% increase over 2020. This surge has been followed by growing trends in ransomware and social engineering attacks, enabled by preventable vulnerabilities such as poor system configuration, human error, and unpatched software.[6]

45. High-profile data breaches at major corporations in recent years have demonstrated that companies holding large volumes of sensitive consumer data are increasingly attractive targets for cybercriminals.

46. In September 2023, Microsoft disclosed that its AI research team inadvertently exposed 38 terabytes of internal data—including passwords, private keys, and internal Teams messages—through a misconfigured Azure cloud storage container.[7] The breach occurred due to an overly permissive Shared Access Signature (SAS) token that allowed full access to the exposed data.

47. Likewise, in July 2023, Estée Lauder was the victim of two ransomware attacks in which threat actors accessed and exfiltrated over 131 GB of corporate data, including email archives and sensitive business files.[8] The incident was linked to the MOVEit file transfer vulnerability exploited globally throughout 2023.

48. These and similar breaches should have placed Coinbase on heightened notice that

[5] *Id.*
[6] Identity Theft Resource Center, *2021 Annual Data Breach Report*, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/
[7] See Ravie Lakshmanan, Microsoft AI Researchers Accidentally Expose 38TB of Private Data via GitHub, *The Hacker News* (Sept. 18, 2023), https://thehackernews.com/2023/09/microsoft-ai-researchers-accidentally.html.
[8] See Scott Ikeda, Two Ransomware Gangs Hack Beauty Giant Estée Lauder, Leaking 131 GB via a MOVEit Data Breach, *CPO Magazine* (July 25, 2023), https://www.cpomagazine.com/cyber-security/two-ransomware-gangs-hack-beauty-giant-estee-lauder-leaking-131-gb-via-a-moveit-data-breach.

any company aggregating sensitive PII—particularly in the financial and crypto sectors—is at significant risk of being targeted. As one of the world's largest digital asset exchanges, Coinbase knew or should have known that it was operating in a high-threat environment and was therefore obligated to implement and maintain best-in-class cybersecurity measures to protect its users' data.

49. Federal law enforcement, including the FBI and U.S. Secret Service, has issued repeated warnings to businesses regarding the rise of ransomware and data exfiltration schemes. These agencies stress the importance of preventive defense and incident response preparedness for organizations that handle personal data.[9]

50. As explained by the FBI, ransomware is a form of malicious software that encrypts or steals data and demands payment to restore access. The FBI strongly advises against paying ransom, as it rarely results in full data recovery and instead incentivizes further criminal activity.[10] The agency emphasizes the need for strong preventive measures, including encryption, security audits, and staff training.

51. Despite widespread awareness of cybersecurity threats and its own role as a financial data custodian, Coinbase failed to take appropriate precautions to secure Plaintiff's and Class Members' PII. The company reportedly stored sensitive data in a manner that was either not properly encrypted or was inadequately protected, thereby enabling unauthorized access during the breach. may not have been encrypted and failed to offer credit monitoring or other post-breach remediation.[11] These omissions demonstrate a reckless disregard for user security and a violation of Coinbase's legal and ethical duties.

D. The Value of Personal Information and the Consequences of Unauthorized Disclosure

[9] U.S. Secret Serv. & Fed. Bureau of Investigation, *Ransomware Trends and Mitigation* (Joint Advisory, 2021), https://www.cisa.gov/sites/default/files/publications/ransomware-advisory-2021.pdf.
[10] Fed. Bureau of Investigation, *Ransomware: What It Is and What to Do About It*, https://www.fbi.gov/investigate/cyber/ransomware.
[11] Owen Hughes, *Coinbase Says Data Stolen by Rogue Support Agent in Ransom Attempt*, TECHREPUBLIC (May 2025), https://www.techrepublic.com/article/news-coinbase-data-breach/.

52. At all relevant times, Coinbase was well aware that the personal information it collected from Plaintiff and Class Members—including names, contact information, partial Social Security numbers, bank account details, and government-issued ID images—was highly sensitive and valuable to cybercriminals.

53. PII is a valuable commodity in illicit markets. The FTC has recognized that identity thieves can use PII to commit a wide array of crimes, including credit and bank fraud, tax fraud, medical identity theft, and government benefits fraud.[12] Stolen PII is routinely bought and sold on the dark web, often in bulk, and can be reused for years to perpetrate identity-based crimes.

54. The consequences of Coinbase's failure to safeguard Plaintiff's and Class Members' PII are long-lasting and severe. Once compromised, this information cannot be "returned" or fully protected. Victims often face fraud risks for years following a breach, as identity thieves delay use of stolen data or circulate it over time in criminal marketplaces.

55. Studies show that approximately 21% of identity theft victims are unaware their information has been misused until two years or more after the compromise, underscoring the extended danger period victims face.[13] In many cases, victims only discover the theft when they receive debt collection notices, erroneous medical bills, or denials of credit.

56. Unlike many companies responding to similar breaches, Coinbase did not offer identity theft protection services or credit monitoring to affected individuals. This failure places the burden squarely on Plaintiff and Class Members to detect and respond to fraudulent activity—activity caused by Coinbase's own data security failures.

57. Coinbase's lack of post-breach support is especially inadequate given the severity of the breach and the long-term nature of the risks. Even if such services had been offered, short-

[12] 16 C.F.R. § 603.2(a)–(b) (2023).
[13] Javelin Strategy & Research, 2021 Identity Fraud Study: Shifting Angles (Mar. 23, 2021), https://javelinstrategy.com/research/2021-identity-fraud-study-shifting-angles.

term monitoring is insufficient to protect against the enduring exposure to fraud that follows the compromise of immutable identifiers like Social Security numbers and government-issued IDs.

58. As a result, Plaintiff and Class Members are left without meaningful tools to mitigate the threat of identity theft, and without compensation for the time, money, and emotional distress they will continue to endure in attempting to safeguard their financial lives.

59. The injuries sustained by Plaintiff and Class Members were directly and proximately caused by Coinbase's failure to implement and maintain reasonable and appropriate data security measures. Coinbase's misconduct has exposed Plaintiff and Class Members to a foreseeable, substantial, and continuing risk of harm.

E. Coinbase Failed to Comply with FTC Data Security Standards

60. Coinbase's handling of users' personal information failed to meet the standards set forth by the FTC for businesses that collect and store sensitive consumer data. Under the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, companies are prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has consistently held that a company's failure to implement reasonable and appropriate data security measures for consumer information constitutes an "unfair practice" under Section 5 of the FTC Act.[14]

61. The FTC has issued extensive guidance emphasizing that data security must be a core consideration in all business operations that involve consumer data. In particular, the FTC expects companies to adopt security measures appropriate to the sensitivity of the data they collect, and to continually evaluate and address emerging threats and vulnerabilities.

62. In 2016, the FTC published Protecting Personal Information: A Guide for Business, which outlines specific practices that companies should follow to secure customer data. These

[14] 15 U.S.C. § 45(a)(1); *see also* Fed. Trade Comm'n, *Privacy & Security Enforcement: Data Security*, https://www.ftc.gov/business-guidance/privacy-security/data-security (last visited May 16, 2025).

include: encrypting information stored on company networks, properly disposing of data no longer needed, understanding and mitigating network vulnerabilities, and developing and enforcing written information security policies.[15]

63. The FTC also advises companies to avoid retaining sensitive information longer than necessary, limit internal access to private data, require the use of complex passwords and multi-factor authentication, regularly monitor networks for suspicious activity, and ensure that third-party vendors implement comparable security standards.

64. The FTC has brought numerous enforcement actions against companies that failed to meet these expectations. In *FTC v. Wyndham Worldwide Corp*., for example, the Third Circuit upheld the FTC's authority to penalize companies that do not take reasonable steps to secure consumer information.[16] These enforcement actions confirm that neglecting to safeguard sensitive personal data—particularly when it leads to a breach—is a recognized violation of federal law.

65. Coinbase's failure to implement and maintain reasonable security measures—despite collecting highly sensitive personal and financial information from millions of users—falls squarely within the scope of the FTC's enforcement authority. Its conduct constituted an unfair practice that exposed Plaintiff and Class Members to a foreseeable and preventable risk of identity theft and fraud.

F. Coinbase's Inadequate Security Caused Concrete Injuries to Plaintiff and the Class

66. Coinbase collected and stored highly sensitive personal information from Plaintiff and Class Members—including names, mailing addresses, email addresses, bank account information, Social Security numbers, and government-issued identification—as a condition of using its cryptocurrency trading and custody platform. Coinbase was entrusted with this data based

[15] Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.
[16] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 245–47 (3d Cir. 2015).

on an expectation that it would maintain industry-standard protections.

67. Plaintiff and Class Members reasonably expected that Coinbase would take adequate steps to protect their personal information from unauthorized access. The decision to open and maintain accounts with Coinbase was predicated, in part, on Coinbase's representations and public-facing policies concerning the security of user data.

68. Coinbase's failure to implement reasonable data security measures deprived Plaintiff and Class Members of the benefit of their bargain. In exchange for providing sensitive personal information and transacting through Coinbase's platform, users expected that their data would be securely stored. Instead, Coinbase's deficient security practices rendered that information vulnerable to theft. As a result, Plaintiff and Class Members received services of materially diminished value and suffered pecuniary harm.

69. The cybercriminals responsible for the May 2025 data breach targeted Coinbase precisely because of the volume and sensitivity of its user data. That stolen information—already confirmed to include identifying details and government ID images—now places Plaintiff and Class Members at a persistent and elevated risk of identity theft, fraud, and future economic loss.

70. Data of this kind is routinely sold on dark web marketplaces, where buyers use it to engage in various forms of fraud. Once sold, this data may be repeatedly resold, repackaged, and combined with other breached datasets to enhance its utility for malicious actors.

71. With access to the PII compromised in the breach, identity thieves can:

- Obtain employment under false pretenses;
- Apply for and secure loans in the victim's name;
- Open credit card accounts or use credentials for fraudulent purchases;
- File false tax returns and claim refunds;
- Steal government benefits, including unemployment or Social Security payments; and

- Apply for driver's licenses, passports, or other government-issued IDs using stolen credentials.

72. In more severe cases, criminals may use a Class Member's stolen Social Security number and personal information to create false identities used in the commission of crimes. This can lead to wrongful criminal records being created in victims' names, complicating future background checks, employment, housing, and loan approvals.

73. As a direct and proximate result of Coinbase's wrongful acts and omissions, Plaintiff and Class Members have suffered the loss of control over and the diminished value of their personal information. PII has an established value in national and international markets and is treated as a tradeable commodity among cybercriminals.

74. The long-term risk is especially acute because PII has a long "shelf life." It is not easily changeable and can be used indefinitely across multiple platforms and sectors. Because identity theft often takes months or years to detect, victims remain vulnerable long after the initial breach.

75. Coinbase's misconduct has thus placed Plaintiff and Class Members at an immediate, ongoing, and heightened risk of identity theft, financial fraud, and other personal and economic harms.

76. As a result of the breach, Plaintiff and Class Members have already suffered concrete injuries, including out-of-pocket expenses, lost time, loss of privacy, emotional distress, and ongoing exposure to substantial and imminent future harm.

V. CLASS ALLEGATIONS

77. Plaintiff brings this class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

78. The Class that Plaintiff seeks to represent is defined as follows:

Nationwide Class:
All individuals residing in the United States whose Private Information was maintained by Coinbase and was exposed to unauthorized third parties in the Data Breach.

79. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers, and directors, current or former employees, and subcontractor used by Defendants in performing its duties; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

80. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate, including but not limited sub-classes and/or state-specific classes depending on evidence and information learning during discovery.

81. **Numerosity, Fed R. Civ. P. 23(a)(1)**: The Class is so numerous that joinder of all members is impracticable. The Class includes thousands of individuals whose Private Information may have been improperly accessed in the Data Breach.

82. **Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3)**: Questions of law and fact common to the Class predominate over any questions affecting only individual Class Members. These include:

a. Whether and when Defendants actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendants owed a duty to the Class to exercise due care in

collecting, storing, safeguarding and/or obtaining their Private Information;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff and Class Members' Private Information;

e. Whether Defendants acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class Members' PII;

f. Whether Defendants knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class Members' PII secure and prevent loss or misuse of that Private Information;

g. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendants caused Plaintiff's and Class Members' damages;

i. Whether Defendants violated the law by failing to promptly notify Class Members that their Private Information had been compromised;

j. Whether Plaintiff and the other Class Members are entitled to actual damages, credit monitoring, and other monetary relief;

k. Whether Defendants violated common law and statutory claims alleged herein

83. **Typicality, Fed. R. Civ. P. 23(a)(3)**: Plaintiff's claims are typical of those of other Class Members, because all had their Private Information compromised as a result of the Data Breach, due to Defendants' misfeasance.

84. **Adequacy, Fed. R. Civ. P. 23(a)(4)**: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that

would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

85. **Superiority and Manageability, Fed. R. Civ. P. 23(b)(3)**: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

86. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since Defendants would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is similar to that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and

duplicative of this litigation.

87. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

88. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

89. **Predominance.** The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Defendants have engaged in a common course of conduct toward Plaintiffs and Class members. The common issues arising from Defendants' conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these issues in a single action has important and desirable advantages of judicial economy.

CAUSES OF ACTION

Count I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class)

90. Plaintiff re-alleges and incorporates by reference the paragraphs 1 through 89 above as if fully set forth herein.

91. Defendants gathered and stored the Private Information of Plaintiff and Class Members as part of the regular course of its business operations. Plaintiff and Class Members were entirely dependent on Defendants to use reasonable measures to safeguard their Private Information and were vulnerable to the foreseeable harm described herein should Defendants fail to safeguard their Private Information.

92. By collecting and storing this data in its computer property, and sharing it, and

using it for commercial gain, Defendants assumed a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

93. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

94. Defendants had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

95. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

96. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

97. Defendants gathered and stored the Private Information of Plaintiff and Class Members as part of its business of soliciting its services to its clients and its clients' patients, which solicitations and services affect commerce.

98. Defendants violated the FTC Act by failing to use reasonable measures to protect

the Private Information of Plaintiff and Class Members and by not complying with applicable industry standards, as described herein.

99. Defendants breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class Members' Private Information, and by failing to provide prompt notice without reasonable delay.

100. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and those who received its services, which is recognized by laws and regulations, as well as common law.

101. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

102. Defendants' multiple failures to comply with applicable laws and regulations constitute negligence per se.

103. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations, but also because Defendants are bound by industry standards to protect confidential Private Information.

104. Defendants had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

105. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class members had no ability to protect their Private Information that was in Defendants' possession.

106. Defendants were in a special relationship with Plaintiff and Class Members with respect to the hacked information because the aim of Defendants' data security measures was to

benefit Plaintiff and Class Members by ensuring that their personal information would remain protected and secure. Only Defendants were in a position to ensure that their systems were sufficiently secure to protect Plaintiff' and Class Members' Private Information. The harm to Plaintiff and Class members from its exposure was highly foreseeable to Defendants.

107. Defendants owed Plaintiff and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

108. Defendants' duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

109. Defendants had duties to protect and safeguard the Private Information of Plaintiff and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendants owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendants' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiff and Class Members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their Private Information.

110. Only Defendants were in a position to ensure that its systems and protocols were sufficient to protect the Private Information that had been entrusted to them.

111. Defendants breached its duties of care by failing to adequately protect Plaintiff' and Class Members' Private Information. Defendants breached their duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;

d. Failing to adequately train its employees to not store Private Information in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff' and Class Members' Private Information;

f. Failing to mitigate the harm caused to Plaintiff and the Class Members;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify Plaintiff and Class Members of the Data Breach that affected their Private Information.

112. Defendants' willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

113. As a proximate and foreseeable result of Defendants' grossly negligent conduct,

Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

114. Through Defendants' acts and omissions described herein, including but not limited to Defendants' failure to protect the Private Information of Plaintiff and Class Members from being stolen and misused, Defendants unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Class Members while it was within Defendants' possession and control.

115. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendants prevented Plaintiff and Class Members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

116. As a result of the Data Breach, Plaintiff and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to the fraudulent use of the Private Information, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

117. Defendants' wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

118. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendants' grossly negligent conduct.

119. Plaintiff and the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

Count II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class)

120. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 89 above as if fully set forth herein.

121. Plaintiff and Class Members were required to provide their PII to Defendants as a condition of owning a franchise or doing business with the Defendants.

122. Plaintiff and Class Members provided their PII to Defendants in exchange for Defendants' services. In exchange for the PII, Defendants promised to protect their PII from unauthorized disclosure.

123. At all relevant times Defendants promulgated, adopted, and implemented written a Privacy Policy whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

124. On information and belief, Defendants further promised to comply with industry standards and to make sure that Plaintiff' and Class Members' Private Information would remain protected.

125. Implicit in the agreement between Plaintiff and Class Members and the Defendants to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

126. When Plaintiff and Class Members provided their Private Information to Defendants as a condition of relationship, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

127. Defendants required Class Members to provide their Private Information as part of Defendants' regular business practices.

128. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

129. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

130. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

131. Defendants breached their implied contracts with Class Members by failing to safeguard and protect their Private Information.

132. As a direct and proximate result of Defendants' breaches of the implied contracts, Class Members sustained damages as alleged herein.

133. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

134. Plaintiff and Class Members are also entitled to nominal damages for the breach of implied contract.

135. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long term credit monitoring to all Class Members for a period longer than the grossly inadequate one-year currently offered.

Count III
INVASION OF PRIVACY

(On behalf of Plaintiff and the Nationwide Class)

136. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 89 above as if fully set forth herein.

137. Plaintiff and the Class Members have a legally protected privacy interest in their Private Information, which is and was collected, stored, and maintained by Defendants, and they are entitled to the reasonable and adequate protection of their Private Information against foreseeable unauthorized access, as occurred with the Data Breach.

138. Plaintiff and the Class Members reasonably expected that Defendants would protect and secure their Private Information from unauthorized parties and that their Private Information would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

139. The Defendants unlawfully invaded the privacy rights of Plaintiff and the Class Members by engaging in the conduct described above, including by failing to protect their Private Information by permitting unauthorized third parties to access, exfiltrate and view this Private Information. Likewise, Defendants further invaded the privacy rights of Plaintiff and Class Members and permitted cybercriminals to invade the privacy rights of Plaintiff and Class Members, by unreasonably and intentionally delaying disclosure of the Data Breach, and failing to properly identify what Private Information had been accessed, exfiltrated, and viewed by unauthorized third-parties.

140. This invasion of privacy resulted from Defendants' failure to properly secure and maintain Plaintiff and Class Members' Private Information, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

141. Plaintiff and Class Members' Private Information is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged

with safeguarding it. Further, the public has no legitimate concern in Plaintiff and Class Members' Private Information, and such information is otherwise protected from exposure to the public by various statutes, regulations, and other laws.

142. The disclosure of Plaintiff and Class Members' Private Information to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

143. Defendants' willful and reckless conduct which permitted unauthorized access, exfiltration and disclosure of Plaintiff and Class Members' Private Information is such that it would cause serious mental injury, shame, or humiliation to people of ordinary sensibilities.

144. The unauthorized access, exfiltration, and disclosure of Plaintiff and Class Members' Private Information was without their consent, and in violation of various statutes, regulations, and other laws.

145. As a result of the invasion of privacy caused by Defendants, Plaintiff and Class Members suffered and will continue to suffer damages and injury as set forth herein.

146. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

Count IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class)

147. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 89 above as if fully set forth herein.

148. Plaintiff and Class Members conferred a monetary benefit on Defendants in the form of the provision of their Private Information and Defendants would be unable to engage in their regular course of business without that Private Information.

149. Defendants appreciated that a monetary benefit was being conferred upon it by

Plaintiff and Class Members and accepted that monetary benefit.

150. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendants to retain that benefit without payment of the value thereof. Specifically, Defendants enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to increase their own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite data security.

151. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures.

152. Defendants acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged. If Plaintiff and Class Members knew that Defendants had not secured their Private Information, they would not have agreed to provide their Private Information to Defendants.

153. Plaintiff and Class Members have no adequate remedy at law. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate

the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

154. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

155. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on his own behalf and on behalf of all others similarly situated, pray for relief as follows:

A. For an Order certifying this case as a class action and appointing Plaintiff and his counsel to represent the Class;

B. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

C. For injunctive and other equitable relief to ensure the protection of the sensitive information of Plaintiff and the Class which remains in Defendants' possession;

D. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

E. Pre- and post-judgment interest on any amounts awarded; and

F. Such other and further relief as the Court may deem just and proper.

VII. JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury on all claims so triable.

DATED: May 16, 2025

Respectfully submitted,

/s/ Melissa R. Emert

KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
Melissa R. Emert
Gary S. Graifman
135 Chestnut Ridge Road
Suite 200
Montvale, NJ 07645
Telephone : 201-391-7000
Facsimile : 201-307-1086
memert@kgglaw.com
ggraifman@kgglaw.com

Attorneys for Plaintiff and the Proposed Class